A. Claims 1-10 (U.S. Patent No. 5,958,005 (Thorne) and the Netscape Publication)

Claim 1 is being amended to emphasize that the electronic mail control software automatically replaces, without further intervention by the user, the destination address *selected by the user* with an address of a central server and places the user-selected destination address in a header to be read only by the central server so that the central server can forward the message to the selected recipient.

The Thorne patent discloses an e-mail system in which e-mail is sent directly to the recipient using the address selected by the user, without replacement by the software in the manner claimed. The Netscape publication discloses a way for a user to enter an electronic mail address, but also does not disclose replacement or substitution of the selected electronic mail address.

It is respectfully noted that in an ordinary electronic mail transmission, including those disclosed by Thorne and Netscape (at least there is no indication in either reference to the contrary), the destination address selected by the user is used to route the electronic mail through an e-mail server and various downstream servers. There is no replacement of the destination address, and of course the destination address selected by the user is not packaged so as to be read only by a central server whose destination address has replaced the originally selected electronic mail address.

In the claimed invention, substitution of the central server address is necessary so that the central server can control handling of the electronic mail at the destination address. While the Thorne patent teaches controls that limit handling by the recipient, it does not use a central server to achieve those controls, and thus there is no need for the destination address substitution address substitution claimed.

Corresponding amendments have been made to independent claim 6.

B. Claims 11-14 (U.S. Patent Nos. 6,185,603 (Henderson) and 6,324,569 (Ogilvie))

Independent claims 11 and 14 recite that the viewer applet sent to the recipient by the central server decodes information in the *header* of an e-mail message and chooses which information to present at the option of the sender. The Henderson patent merely discloses display of plaintext messages in the *re* line of a message so that the message can be read without the need to open the e-mail. The program that permits viewing of the e-mail of Henderson does not, as claimed, selected header information for viewing at the option of the *sender*, so that the sender can determine which header information is to be viewed by the *recipient*.

The Ogilvie patent, on the other hand, does not disclose any sort of central server, viewer applet, or encryption of *header* information. Instead, Ogilvie discloses a method and system in which e-mail that is not read is automatically deleted. In the system of Ogilvie, no limitations are placed on viewing of the message by the recipient. Indeed, such controls would be contrary to the purpose of the Ogilvie system, which is to avoid annoying persons who do not wish to read an e-mail by eliminating the need to positively delete the e-mail if deletion is desired. The sender presumably wants recipients to read the e-mail and places absolutely no restrictions on doing so, but merely makes it convenient to automatically delete the e-mail if viewing is not desired. In contrast, the claimed invention forces deletion even if viewing is desired, which is exactly contrary to Ogilvie.

To further emphasize that claims 11 and 14 involve *header* information, claims 11 and 14 have been amended to identify specific header information affected, namely sender-identity and message-origination information.

C. Claims 15-24 (Henderson, Ogilvie, and U.S. Patent 6,061,448 (Smith))

These claims are directed to the overall system of involving use of a central e-mail server to control viewing by the recipient. This is different than, for example, an ordinary encrypted e-mail in which various servers, including a destination e-mail server, might handle the e-mail message as it is sent from the source to the destination, but in which none of the servers that

handles the e-mail as it is routed from source to destination encrypts the message at the request of the sender, and then send the electronic mail message to a viewer applet installed on the recipient computer *so that the message can be viewed only by using the viewer applet and a session key* [which is a different type of encryption than public key encryption, and which involves shared secret keys and a two-way dialog between the viewer applet and the central server in order to develop the "session key"], in order to implement controls requested by the original sender. Neither the *re* line viewer of Henderson nor the spam elimination method of Ogilvie (nor the postage dispenser of U.S. Patent No. 6,005,945 (Whitehouse)) suggests any of the above-described positively recited features of the invention.

With respect to the Smith patent applied against claims 20 and 23, while the claimed invention can use public key encryption as taught by Smith, public key encryption *per se* is not being claimed. Instead, the claims are directed to a *header* viewing system and method that happens to use encryption, but that does so in a way that is not suggested by either Henderson or Ogilvie, namely encryption of header information so that a viewer on the recipients computer can prevent, at the option of the sender, viewing of certain header information such as the identity of the sender and time and place of message origination. Neither Henderson nor Ogilvie even remotely discloses or suggests these aspects of the claimed invention.

D. Claims 25-30 (U.S. Patent Nos. 5,864,684 (Nielson); 6,442,600 (Anderson); *et al.*)

Claims 25-30 are directed to a system and method by which electronic mail lists can be expanded to persons unknown to the original sender (or server). This feature is not suggested by any of the five U.S. Patents cited in items 11 and 12 of the Official Action.

Because the system of the invention uses a central mail server to control handling of an e-mail by a recipient, it controls forwarding of the message. A side effect of this control is that it can monitor the identity of persons to whom the original recipients forward the e-mail, and control forwarding by those new recipients *even though the identity of the new recipients was previously unknown to the sender.* This goes way beyond the capabilities of a system of the type

disclosed in the Nielson patent, which simply prevents forwarding, or the Sidhu patent, which monitors e-mail activity persons connected to a network. A network server such as the one disclosed in the Sidhu patent inherently knows who is on the network, and also can monitor initial recipients of e-mails sent by persons on the network, *but cannot track e-mails sent by persons to whom e-mail is forwarded by the initial recipients*.

The claimed system and method can expand an initial recipient list to every person who receives *and reads* the initial e-mail message, even if the message has been forwarded numerous times, because the forwarded e-mail messages can only be read if an appropriate viewer applet is used, the viewer applet reporting back to the central server on whether the e-mail is read.

2. Why Amendments Should Be Entered

It is respectfully submitted that the amendments presented below merely emphasize features already recited in the original claims, and that the arguments made above apply to the original as well as to the amended claims.

Therefore, the amendments do not raise new issues, and entry of the amendments is respectfully requested.

For the reasons given above and during the interview, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,
BACON & THOMAS, PLLC

Date: May 23, 2003

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500

APPENDIX B
(Marked-Up Copy Of Claims)

1. (Twice Amended) Electronic mail control software, comprising:

means for opening a window arranged to enable a user of the electronic mail applications program to select

(i) an original destination address to which an electronic mail message created using the electronic mail applications program is to be sent, and

(ii) control options to be applied to the electronic mail message; and

means for causing the electronic mail control software to automatically substitute, without manual entry of a substitute address by the user, an address of a central mail server for the original destination address selected by the user in order to divert said electronic mail message to [a] said central mail server, said original destination address being appended by the electronic mail control software to the message so that it can be read by the central mail server, the central mail server being arranged to forward said electronic mail message to said original destination address and to implement said control options if one of said control options is selected.

2. (Unchanged) Electronic mail control software as claimed in claim 1, wherein said control options include an expiration setting by which the user may select a date, time, or event, the occurrence of which will cause said message to expire.

3. (Unchanged) Electronic mail control software as claimed in claim 1, wherein said control options include limitations on forwarding by a recipient of said message.

4. (Unchanged) Electronic mail control software as claimed in claim 1, wherein said means for opening said window includes means for intercepting a send command generated by said electronic mail applications program and opening said window in response to interception of said send command.

5. (Unchanged) Electronic mail control software as claimed in claim 1, further comprising means for modifying at least one entry in an address book of said electronic mail applications program to cause mail sent to said entry to be routed through said electronic mail server.

6. (Amended) A method of adding lifespan and handling limitations to an electronic mail message, comprising the step of:

opening a window arranged to enable a user of the electronic mail applications program to select

(i) an original destination address to which an electronic mail message created using the electronic mail application program is to be sent, and

(ii) control options to be applied to the electronic mail message,

wherein, when one of said control options is selected by the user, the electronic mail [applications] application program automatically substitutes, without further entry of an address by the user, an address of a central mail server for the original destination address and appends the original destination address to the electronic mail message in order to divert the electronic mail message to a central mail server arranged to read the original destination address and forward the electronic mail message to said original destination address and to implement said control options.

7. (Unchanged) A method as claimed in claim 6, wherein said control options include an expiration setting by which the user may select a date, time, or event, the occurrence of which will cause said message to expire.

8. (Unchanged) A method as claimed in claim 6, wherein said control options include limitations on forwarding by a recipient of said message.

9. (Unchanged) A method as claimed in claim 6, wherein the step of opening said window includes the step of intercepting a send command generated by said electronic mail applications program and opening said window in response to interception of said send command.

10. (Unchanged) A method as claimed in claim 6, further comprising the step of modifying at least one entry in an address book of said electronic mail applications program to cause mail sent to said entry to be routed through said electronic mail server.

11. (Twice Amended) An electronic mail system, comprising:

a first computer on which is installed message origination software and which is connected to a network capable of carrying an electronic mail wrapper that includes an electronic mail message;

B1

at least one recipient computer also connected to said network; and

a viewer applet installed on said recipient computer,

said viewer applet being arranged to decode control information appended to the electronic mail wrapper, search for sender-identity and message-origination fields in said wrapper and control, based on input to said message origination software, a manner in which information items in said [selected] sender-identity and message-origination fields in said wrapper are presented to a recipient of the message, said control including selection of which of said information items in said sender-identity and message-origination fields are to be presented, and control of coupling of the information and the message.

12. (Unchanged) An electronic mail system as claimed in claim 11, further comprising a central electronic mail server connected to said network, said electronic mail server being arranged to cooperate with said viewer applet to achieve said control of the manner in which the electronic mail wrapper is presented to the recipient.

13. (Unchanged) An electronic mail system as claimed in claim 12, wherein upon request by the recipient, said central mail server encrypts said electronic mail message and sends it to said viewer applet, and said viewer applet being arranged to decrypt said message so as to display said message with information deleted from said wrapper.

57

B

14. (Twice Amended) A method of controlling an electronic mail message transmitted over a network,

comprising the steps of:

after transmission of the electronic mail message over the network, identifying and selecting information in sender-identity and message-origination fields of a message wrapper associated with the electronic mail message; and

encrypting said electronic mail message so that only said selected information in said sender-identity and message-origination fields in said associated message wrapper can be viewed with the message when the electronic mail message is decrypted using a viewer applet installed on a recipient computer.

15. (Amended) A method of controlling an electronic mail message transmitted over a network, comprising the steps of:

before transmission of the electronic mail message over the network, [attaching] enabling a user to attach limitations on processing and handling of the electronic mail message by a recipient;

initially transmitting said electronic mail message over said network to a central electronic mail server;

storing said electronic mail message at said electronic mail server;

upon request by the recipient, [encrypting] causing said electronic mail server to encrypt said electronic mail message[,];

[sending] causing the electronic mail server to send the encrypted electronic mail message to a viewer applet installed on said recipient computer[, and];

[storing] causing the viewer applet to store said encrypted message on the recipient computer;

causing the viewer applet to enable viewing of said message by decrypting said electronic mail message using the viewer applet and a session key supplied by the central electronic mail server, wherein said message cannot be viewed by the recipient unless the viewer applet is used; and

causing said central electronic mail server and viewer applet to implement said processing and handling limitations.

16. (Unchanged) A method as claimed in claim 15, wherein said session key is supplied by said central server each time said message is to be viewed.

17. (Unchanged) A method as claimed in claim 15, wherein said session key must be renewed periodically in order to view said message.

18. (Amended) A method as claimed in claim 15, wherein said viewer applet is required to establish communications with the central server periodically in order to ensure that a clock used by the viewer applet is functioning properly.

19. (Amended) An electronic mail system, comprising:

a first computer on which is installed message origination software arranged to assign message processing limitations to an electronic mail message and which is connected to a network capable of carrying said electronic mail message;

at least one recipient computer also connected to said network;

a viewer applet; and

a central electronic mail server connected to said network, said message origination software being arranged to send said electronic mail message to said electronic mail server, said electronic mail server being arranged to store information concerning said electronic mail message and, upon request by the recipient, encrypt said electronic mail message and send it to said viewer applet, wherein said viewer applet is arranged to decrypt said viewer applet as it is sent so as to display said message,

wherein said viewer applet is also arranged to store at least a portion of said message that has been stripped of said information by said central server,

wherein said message can only be viewed by the recipient using the viewer applet, and

wherein said processing limitations are implemented by said central electronic mail server and said viewer applet.

20. (Unchanged) An electronic mail system as claimed in claim 19, wherein said message is encrypted by said central mail server using a public key generated by the viewer applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

21. (Unchanged) An electronic mail system as claimed in claim 19, wherein said viewer applet is further arranged to permit a user to request forwarding of said electronic mail message to a second recipient computer, said central mail server being arranged to strip and store information concerning said message, a copy of the viewer applet installed on said second recipient computer being arranged to store said stripped message.

22. (Amended) A method of controlling an electronic mail message transmitted over a network, comprising the steps of:

before transmission of the electronic mail message over the network, attaching limitations on processing and handling of the electronic mail message by a recipient;

initially transmitting said electronic mail message over said network to a central electronic mail server;

storing said electronic mail message at said electronic mail server;

upon request by the recipient, encrypting said electronic mail message, sending the encrypted electronic mail message to a viewer applet installed on said recipient computer, and decrypting said electronic mail message as it is received by the viewer applet so as to display said message; and

causing said central server and viewer applet to implement said processing and handling limitations.

23. (Amended) A method of controlling an electronic mail message as claimed in claim 22, further comprising the steps of encrypting said electronic mail message is carried out by said central electronic mail server using a public key generated by the viewer applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

24. (Amended) A method of controlling an electronic mail message as claimed in claim 22, further comprising the steps of causing said viewer applet to request forwarding of said electronic mail message stored on said central mail server to a second recipient computer, encrypting said electronic mail message using a public key of a copy of said viewer applet installed on said second recipient computer, and sending said stripped electronic message to said second recipient computer for storage in a memory of the second recipient computer.

25. (Amended) A method of developing mailing lists, comprising the steps of:

sending an electronic mail message to an initial list of recipients;

requiring that versions of said electronic mail message that are forwarded to first additional recipients by said initial recipients be routed through at least one central mail server, said first additional recipients including recipients initially unknown to the sender and the central mail server;

requiring that versions of said electronic mail message that are forwarded to second additional recipients by said first additional recipients be routed through said at least one central mail server, said second additional recipients including further recipients initially unknown to the sender and the central mail server;

tracking all transactions involving said electronic mail message, including transactions by said original recipients, said first additional recipients, and said second additional recipients; and

using a record of at least a portion of said transactions to expand said electronic mailing list to recipients not on the initial mailing list, and not initially known to the sender or to the central mail server.

26. (Amended) A method as claimed in claim 25, further comprising the steps of: before initial transmission of said message, attaching handling limitations to said message; and encrypting said message so that it can only be viewed by a viewer applet supplied by said central server.

27. (Amended) A method as claimed in claim 25, further comprising the steps of: before transmission of the electronic mail message over an open network, attaching to the message a date, time, or event, the occurrence of which will cause said electronic mail message and all designated incarnations thereof to expire; and encrypting said electronic mail message so that it can only be viewed before the occurrence of said time, date, or even using a viewer applet installed on a recipient computer.

28. (Amended) A method as claimed in claim 25, wherein said record includes all addresses to which said message has been forwarded.

29. (Amended) A method as claimed in claim 25, wherein said record includes a subset of the addresses to which said message has been forwarded.

30. (Amended) A method as claimed in claim 25, further comprising the step of selling said expanded list.